IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

COSMOKEY SOLUTIONS GMBH & CO. KG, Plaintiff, v. DUO SECURITY, INC. n/k/a DUO SECURITY LLC and CISCO SYSTEMS, INC., Defendants.	C.A. No. 18-1477 (JLH) (CJB) REDACTED - PUBLIC VERSION

DEFENDANTS' OPENING BRIEF IN SUPPORT OF THEIR MOTION TO EXCLUDE CERTAIN OPINIONS OF DR. ERIC COLE

OF COUNSEL:

Brian A. Rosenthal
Katherine Dominguez
Allen Kathir
Hyunjong Ryan Jin
Charlie Sim
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
(212) 351-4000

Jaysen S. Chung
Julian Manasse-Boetani
GIBSON, DUNN & CRUTCHER LLP
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
(415) 393-8200

Nathaniel R. Scharn
GIBSON, DUNN & CRUTCHER LLP
3161 Michelson Drive, Suite 1200
Irvine, CA 92612-4412
(949) 451-3800

MORRIS, NICHOLS, ARSHT & TUNNELL LLP
Jennifer Ying (#5550)
Travis J. Murray (#6882)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jying@morrisnichols.com
tmurray@morrisnichols.com

Attorneys for Defendants Duo Security LLC f/k/a Duo Security, Inc. and Cisco Systems, Inc.

Original filing date: December 20, 2024
Redacted filing date: January 7, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Rules

TABLE OF EXHIBITS

Ex.	Description
1	Transcript for December 16, 2024 Deposition of Dr. Eric Cole (excerpts)
2	IPR2019-01638, POPR
3	U.S. Patent No. 9,246,903
4	CosmoKey's May 1, 2023 Infringement Contentions (excerpts)
5	CosmoKey's November 13, 2023 Infringement Contentions (excerpts)
6	Transcript for April 12, 2024 Claim Construction Hearing (excerpts)
7	Transcript for April 15, 2024 Teleconference Regarding the Court's Claim Construction Rulings (excerpts)
8	CosmoKey's May 10, 2024 Infringement Contentions (excerpts)
9	CosmoKey's November 22, 2024 Infringement Contentions (excerpts)
10	Dr. Eric Cole's September 20, 2024 Opening Report
11	Dr. Eric Cole's November 15, 2024 Reply Report
12	Transcript for December 5, 2024 Deposition of Dr. Benjamin Goldberg (excerpts)

I. INTRODUCTION

CosmoKey faces the impossible challenge of trying to come up with an infringement theory that allows it to read the asserted claims on precisely the same type of authentication method that it distinguished in the IPR to avoid institution. Ex. 1 at 128:18–134:9, 142:3–148:8; Ex. 2 at 17–19. Specifically, just like the prior art methods that CosmoKey distinguished in the IPR, Defendants' accused products perform authentication by pushing to the user's mobile device a notification that requires the user to approve or deny the transaction.

To try to make this balancing act work—which CosmoKey fails to do—CosmoKey's infringement expert, Dr. Eric Cole, must concoct an arbitrary, wholly unsupported, and thus legally wrong construction of the claim term "authentication function." In particular, he contends that "authentication function" should be construed as "software elements needed to authenticate." His vague and unexplained construction finds no support in and is inconsistent with the patent, which describes only two categories of embodiments for the term: (1) a hardware component within a mobile device (*i.e.*, a transceiver or SIM card) or (2) an applet, each of which must be activated and deactivated. Under his construction, the "authentication function" can be neither, and instead is something the patent does not contemplate at all: a source code "function," a term of art that refers to a block of source code that, when executed, performs a task.

Dr. Cole's attempt to improperly stretch the term's scope is by design. CosmoKey scrambled to shift infringement theories after the Court correctly held the claims require the "authentication function" to be "*locally* activated at the mobile device by the user." D.I. 180. Based on that ruling, CosmoKey could no longer maintain its old theory that the Duo Mobile App (or applet) itself is the "authentication function" because the App is activated *remotely* by a user choosing at a computer to send a push notification to the App. Once received in the App, the push notification gives the user the option to "approve" or "deny" the request.

Thus, as disclosed for the first time with any clarity in his reply report, Dr. Cole uses his construction to artificially parse the App into sub-parts and accuse as the "authentication function" a later point in the process where the user *locally* interacts with (but does not activate) the App. Specifically, he accuses source code blocks that execute *after* a user selects "approve." At the same time, however, Dr. Cole arbitrarily excludes code blocks that must execute *before* the user makes this selection—because they execute as a result of *remote* user action. But these code blocks also are undeniably—and admittedly—"needed to authenticate" and perform functionality that CosmoKey accused as the "authentication function" before the Court's claim construction ruling.

The patent does not contemplate that the recited "authentication function" can be merely an arbitrary block of source code. Indeed, the patent does not contemplate an "authentication function" that is anything other than (1) a hardware component within a mobile device or (2) an applet. Thus, Dr. Cole's construction, which also excludes disclosed hardware embodiments and allows the "authentication function" to be anything in software that CosmoKey wants it to be with no meaningful bounds, is wrong as a matter of law. His construction and opinions employing it are not the product of reliably applied principles, will mislead the jury, and should be excluded.

II. NATURE AND STAGE OF THE CASE

Fact and expert discovery are closed. A 5-day jury trial is set to begin on June 9, 2025.

III. BACKGROUND

A. The "Authentication Function"

Central to the asserted claims is an "authentication function" "implemented in a mobile device of [a] user." Ex. 3 ('903 patent), cl. 1. Among other limitations, the claims require that this "authentication function" "is activated by the user only preliminarily" for an authentication and is then "automatically deactivated." *Id.* Critical to the claimed method is confirming that the "authentication function" is active, *i.e.*, authentication may proceed only if the "authentication

function" is detected to be active. *See, e.g.*, *id.* at 5:1–9, 5:26–35, 5:46–60, 5:61–6:13, 6:45–7:3.

The specification's guidance as to what constitutes the "authentication function" is limited to two categories of embodiments: (1) a hardware component within a mobile device (*i.e.*, a transceiver or SIM card) or (2) an applet. In either case, it must be activated and deactivated.

Hardware Component Within a Mobile Device. The patent describes a mobile device with a transceiver that is activated or deactivated by a controller, which is also part of the device. Ex. 3 at 8:32–41. The device also includes an "ON-switch," which "may simply be formed by a button, so that the user may activate the authentication function (*i.e.*, the transceiver 40) by pressing the button." *Id.* at 8:41–45. In addition, the "controller 44 has a self-deactivation function deactivating the transceiver 40 a few seconds after it has been activated." *Id.* at 8:53–55.

In other embodiments, the device has "two SIM cards" that "store different sets of access data" and "each . . . has its own mobile telephone number" that is "assigned to a different one of the types of [a] transaction." Ex. 3 at 9:20–32. The device has "two buttons" "for selectively activating one of the two SIM cards." *Id.* at 9:33–34. The patent explains that "the user may specify the type of transaction he wants to perform by pressing either" button "to activate the related SIM card and, implicitly, the related authentication function." *Id.* at 9:34–38. The specification further explains that "[t]he controller 44 will then automatically deactivate the authentication function (SIM card) after a certain time interval." *Id.* at 9:38–40. Dr. Cole concedes these are hardware embodiments of the "authentication function." Ex. 1 at 105:18–116:14.

Applet. The specification also describes an embodiment where "the authentication function that is implemented in the mobile device 16 may take the form of an applet that can be activated and deactivated independently of" the mobile device. Ex. 3 at 6:59–61. In this scenario, to check the "active or inactive state of" the applet, "it is necessary that the authentication device

18 actually sends a request to the applet in the mobile device 16 and the applet responds to this request when it is active." *Id.* at 6:62–7:1.

B. The Court's Claim Construction Ruling That Precluded CosmoKey's Accusation of the Duo Mobile App as the "Authentication Function"

From CosmoKey's original infringement contentions through claim construction briefing, Defendants' understanding of CosmoKey's infringement theory was that the accused "authentication function" in the accused products was the Duo Mobile App. *See, e.g.*, Ex. 4 (5/1/23 Contentions, Ex. A) at 28–31; Ex. 5 (11/13/23 Contentions, Ex. A) at 48–52 ("Duo MFA includes Duo Push, which, along with Duo Mobile," *i.e.*, the application, "provides this limitation"; "Duo Push is inactive until a request is received, and the push notification is triggered only when a user attempts to log in to a system or application thar [sic] requires Duo Push authentication"). Regardless of what CosmoKey accused, however, it was clear from CosmoKey's infringement contentions that CosmoKey argued the "authentication function" can be activated *remotely* by a user selecting at a terminal (*e.g.*, computer) the Duo Push option, "Send Me a Push," which results in sending a push notification to the App on the user's mobile phone. *See, e.g.*, Ex. 5 at 49 ("Duo Push is inactive until a request is received, and the push notification [sent to the Duo Mobile app] is triggered only when a user attempts to log in to a system or application tha[t] requires Duo Push authentication"), 50–51 (identifying the "Duo Push notification [that] shows up on your screen" in the Duo Mobile app as a result). Once received in the App, the push notification gives the user the option to "approve" or "deny" the request. *Id.*

Thus, one of the core claim construction disputes between the parties was *where* the activation of the "authentication function," which is "implemented in a mobile device of [a] user," must occur. Ex. 3 at cl. 1. Defendants explained that the "authentication function" must be activated *locally* at the mobile device by the user. D.I. 136 (Joint Brief) at 23–26, 28–29.

CosmoKey argued there is no such requirement, and thus activation can be accomplished *remotely* by the user at, for instance, the terminal. *Id.* at 21–23, 26–28.

At the *Markman* hearing, the Court asked CosmoKey to "give [the Court] an idea about what would infringe under your claim construction that wouldn't infringe under [Defendants'] claim construction." Ex. 6 (4/12/24 Tr.) at 37:9–11. While CosmoKey failed to provide a clear answer (*id.* at 37:12-42:1), Defendants reiterated that their construction "would preclude [CosmoKey] from saying that th[e] pop up" on the Duo Mobile App in the user's phone "constitutes activating" the "authentication function" "[b]ecause it wasn't locally activated at the mobile device by the user," and was instead "activated remotely" (*id.* at 45:25–46:6, 46:13–48:18).

The Court agreed with Defendants, holding that the "authentication function" must be "*locally* activated at the mobile device by the user only preliminarily for the transaction."[1] D.I. 180 (Order) at 1; Ex. 7 (4/15/24 Tr.) at 6:13–8:24. This ruling precluded CosmoKey from continuing to accuse the Duo Mobile App as the "authentication function" because, as discussed, even CosmoKey's infringement contentions show that the App is activated *remotely* by the user.

Thus, CosmoKey sought to shift theories to another aspect of the accused products that it could accuse as an "authentication function"—but it then needed to accuse something that is *locally* activated by a user on their mobile device. Although CosmoKey served supplemental infringement contentions in May 2024, it failed to adequately identify what it contended was the accused "authentication function" and thus left unspecified exactly how it would change its infringement theory in light of the Court's construction. Ex. 8 (5/10/24 Contentions). Defendants therefore moved to compel supplemental infringement contentions on that basis in July 2024, and Judge Burke granted the motion on November 13, 2024. D.I. 313 (Order); D.I. 265 & 285 (Defs.

[1] Unless otherwise noted, emphasis has been added to quotes included in this brief.

Opening and Reply Briefs). On November 22, 2024, CosmoKey served supplemental contentions that merely incorporated by reference the opinions in the reports of its infringement expert, Dr. Eric Cole, that had been served in the time between Defendants requesting relief and the Court granting it. Ex. 9 (11/22/24 Contentions) at 2; *see id.*, Ex. A at 41–44.

C. Dr. Cole's Construction of "Authentication Function" and New Infringement Theory

In his opening and reply reports, Dr. Cole opines that [redacted] *See, e.g.*, Ex. 10 (Opening) ¶¶ 206, 276; Ex. 11 (Reply) ¶¶ 70, 74, 82, 97, 102, 108. He does not explain or identify any support for his construction beyond citing portions of the patent concerning an "authentication function" that is (1) a hardware component within a mobile device or (2) an applet—and thus these citations do not actually support his construction. Ex. 10 ¶ 98 (citing '903 patent, 6:59-62, 8:32-37, 9:8-12, 9:20-32); Ex. 11 ¶ 67 (citing '903 patent, 8:32-37, 9:8-12, 9:20-32).

Dr. Cole then employs this construction for his infringement theory, which CosmoKey had not disclosed in any of its infringement contentions. Dr. Cole relies on this construction to accuse as the "authentication function" a mere source code "function," which is a term of art that indisputably refers to a block of source code (or set of instructions) that, when executed, performs a task. Ex. 1 at 117:7–15 (agreeing that a source code "function" is just a "set of instructions that a computer executes"); Ex. 12 (12/5/24 Goldberg Tr.) at 141:2–8 (defining a "source code function" as a "portion of code, a sequence of instructions for the computer to perform" that, when called, "is executed by the processor").

In particular, Dr. Cole accuses as the "authentication function" [redacted] Ex. 11 ¶¶ 74–77; Ex. 1 at 104:23–105:16. But he ignores the source code blocks that are executed *before* the user makes that

selection, such as those that execute for the App to receive the push notification (with the "approve" or "deny" options). Those source code blocks execute as a result of the user *remotely* choosing on their computer to send the push notification (*i.e.*, selecting the "Send Me a Push" option discussed above). As Dr. Cole conceded at deposition, however, receiving the push notification in the App is necessary for the authentication process, *i.e.*, it is "needed to authenticate." Ex. 1 at 236:15–237:4. His concession is consistent with CosmoKey's acknowledgment in its earlier infringement contentions that receiving the push notification in the App is part of the accused products' authentication process. *Supra* Section II.B.

IV. LEGAL STANDARD

Expert testimony is admissible only if it "is based on sufficient facts or data," "is the product of reliable principles and methods," and "the expert's opinion reflects a reliable application of the principles and methods to the facts of the case." Fed. R. Evid. 702; *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 592–93, 597 (1993). The party offering expert testimony "bears the burden of proving that her testimony meets Rule 702's restrictions." *Wirtgen Am., Inc. v. Caterpillar, Inc.*, 715 F. Supp. 3d 587, 592 (D. Del. 2024).

V. ARGUMENT

Dr. Cole's construction of "authentication function" as "software elements needed to authenticate," under which it can be an arbitrary source code block that is merely executed, is wrong as a matter of law and thus should be excluded along with his opinions applying it. His construction finds no support in and is inconsistent with the specification, excludes disclosed hardware embodiments, and would render the claims indefinite. Thus, his construction and related opinions are not the product of reliably applied principles and would mislead the jury.

Courts in this District have excluded expert opinions where, as here, the expert's "testimony improperly applies legal principles, such as those relating to claim construction."

Sprint Commc'ns Co. L.P. v. Cox Commc'ns, 302 F. Supp. 3d 597, 624 (D. Del. 2017). Indeed, a court in this District has recognized that "courts routinely preclude those portions of an expert's report that are premised on a misunderstanding of the law." *Exela Pharma Sciences, LLC v. Eton Pharm., Inc.*, 2022 WL 806524, at *3 (D. Del. Feb. 8, 2022). In *Sprint*, the court excluded portions of an expert report where the expert, "without explanation, . . . construe[d] claim terms." 302 F. Supp. 3d at 624. In particular, the expert had "not explain[ed] why he relied on a definition of" a claim term "to the exclusion of specific examples of" that term "in the specification." *Id.* at 622. The court explained that because the expert thus "improperly applie[d] legal principles," including "those relating to claim construction," the court "ha[d] no confidence that [the expert] 'ha[d] reliably applied the principles and methods to the facts of the case'" and thus his "testimony [was] likely to confuse a jury." *Id.* at 624. Here, Dr. Cole's unexplained construction suffers from the same and additional legal errors, and should therefore be excluded.

Dr. Cole's Construction Finds No Support in, and Is Inconsistent With, the Specification. Not once does the '903 patent contemplate or even hint that, as Dr. Cole contends under his construction, the "authentication function" can be any arbitrary source code block. His construction is legally impermissible for that reason alone.

The specification's disclosures concerning the "authentication function" are limited to two categories of embodiments, neither of which contemplates an "authentication function" that is an arbitrary source code block. *Supra* Section II.A. The *first category* is an "authentication function" that is a hardware component within a mobile device; namely, a transceiver or a SIM card. For instance, the patent describes a device with a transceiver that is activated by pressing an "ON-switch" and is then deactivated using a "controller" with a "self-deactivation function." Ex. 3 at 8:32–45, 8:53–55; *see also id.* at 2:56–60. It also describes a device with two SIM cards that relate

to different types of transactions. *Id.* at 9:20–28. The device has two buttons that a user can press to "selectively activat[e] one of the two SIM cards" depending on "the type of transaction [the user] wants to perform." *Id.* at 9:33–38. A "controller" is then used to "automatically deactivate the authentication function (SIM card)." *Id.* at 9:38–40. The *second category* is an "authentication function" that is an "applet that can be activated and deactivated independently" of the device. *Id.* at 6:59–62. To check if the applet is active or inactive, a request is sent to the applet, which then "responds to this request when it is active." *Id.* at 6:62–7:1.

The '903 patent does not contemplate any other embodiments for the "authentication function," much less what Dr. Cole contends it can be under his construction: an arbitrary source code block. The Federal Circuit repeatedly has rejected constructions that, like Dr. Cole's construction, are not contemplated by the patent. For instance, in *Profectus Technology LLC v. Huawei Technologies Co.*, the Federal Circuit disagreed with the patentee and construed the term "mountable" to require "having a feature for mounting." 823 F.3d 1375, 1380–81 (Fed. Cir. 2016). The court held that the patentee "fail[ed] to pinpoint in the intrinsic record where the patent contemplates a situation where *no* mounting features exist," and that "every embodiment disclosed in the specification" instead "include[d] a feature for mounting." *Id.* Similarly, in *Clare v. Chrysler Group LLC*, the Federal Circuit rejected the patentee's construction of a term relating to the "external appearance" of a pickup truck as requiring "visible hinges and latches," reasoning that the specifications "d[id] not contemplate visible hinges and latches." 819 F.3d 1323, 1325, 1331–32 (Fed. Cir. 2016). Likewise, in *Vederi, LLC v. Google LLC*, the Federal Circuit held that the Patent Trial and Appeal Board erred in construing claims that recited "image frames acquired by an image recording device *moving* along a trajectory" as being limited to a device that "only captures images when it is *not* moving." 813 F. App'x 499, 503–04 (Fed. Cir. 2020). The appeals

court explained that "the specification d[id] not disclose a single embodiment" supporting that understanding and that, instead, "the specification repeatedly contemplates acquisition of image frames by an image recording device that *is in motion*." *Id.* at 504.

Here, Dr. Cole's construction should be rejected for at least the same reasons the Federal Circuit rejected the unsupported constructions in *Profectus*, *Clare*, and *Vederi*. The '903 patent never contemplates that a skilled artisan would have understood an "authentication function" to be "software elements needed to authenticate," where those elements can be any arbitrary source code block. Instead, the patent at most contemplates that the "authentication function" is a hardware component within a mobile device (*i.e.*, transceiver or SIM card) or an applet.

Finally, Dr. Cole's construction is not only unsupported by the specification, but it is also inconsistent with the specification. Dr. Cole's "*software* elements needed to authenticate" construction undeniably excludes the patent's disclosed embodiments in which the "authentication function" is a component within a device, *i.e.*, a transceiver or SIM card—both of which he concedes are *hardware*. Ex. 1 at 107:5–116:14. The Federal Circuit has made clear that "[w]e normally do not interpret claim terms in a way that excludes embodiments disclosed in the specification." *Oatey Co. v. IPS Corp.*, 514 F.3d 1271, 1276 (Fed. Cir. 2008). The court has in some cases "interpreted claims to exclude embodiments of the patented invention where those embodiments are clearly disclaimed in the specification or prosecution history." *Id.* Here, however, Dr. Cole identifies no such disclaimer—there is none.

Additional Legal Error in Dr. Cole's Construction. Further underscoring the legal error in Dr. Cole's construction is that the construction, if permitted, would render the claims indefinite. *See Geneva Pharms., Inc. v. GlaxoSmithKline PLC*, 349 F.3d 1373, 1384 (Fed. Cir. 2003) (rejecting a proposed construction that would have rendered the claims indefinite). The Federal Circuit has

explained that an "[o]pen-ended definition of categories that might or might not possess certain traits cannot provide reasonably certain bounds on the scope" of a claim term. *IQASR LLC v. Wendt Corp.*, 825 F. App'x 900, 906 (Fed. Cir. 2020).

Here, Dr. Cole's construction of "authentication function," under which it can be any arbitrary source code block, is precisely such an "open-ended definition" that "cannot provide reasonably certain bounds on the scope" of the claims and thus would render the claims indefinite. The improper open-endedness of Dr. Cole's construction is exemplified by the way he applies it for infringement. The motive behind his construction is also clear: CosmoKey needs it to artificially parse the Duo Mobile App, which CosmoKey previously accused as the "authentication function," into subparts in a manner that CosmoKey believes will escape the Court's "local activation" ruling. In particular, as detailed below, CosmoKey seeks to accuse only those subparts that allegedly execute as a result of *local* user interaction while ignoring other subparts that execute as a result of *remote* user action on a terminal—even though, as Dr. Cole admits, all of them are "needed to authenticate." Ex. 1 at 233:10–17.

As acknowledged in CosmoKey's prior infringement contentions, and as Dr. Cole concedes, the second-factor authentication process in the accused products does not begin when a user selects "approve" in the Duo Mobile App. Ex. 5 at 48–51; *e.g.* Ex. 1 at 204:13–205:14; 218:19–219:19. For a user to have that option in the first place, the user must choose the Duo Push option, "Send Me a Push," on their computer. Ex. 5 at 49. When the user chooses that Duo Push option on their computer, a push notification with the "approve" or "deny" options is received in the App on the user's mobile device. Only after the push notification is received can the user then choose to "approve" or "deny" the request. *Id.* at 49–51. All of these steps in the authentication process require execution of source code blocks, and are thus "software elements needed to authenticate."

Yet Dr. Cole cherry picks only some of them to accuse as the "authentication function."

Constrained by the Court's claim construction ruling, Dr. Cole accuses only the source code blocks that are executed *after* the user selects "approve" in the App—because they allegedly execute as a result of *local* user interaction. Dr. Cole, however, ignores source code blocks that execute *before* the user makes that selection, such as those that execute to receive the push notification with option to "approve" or "deny" the request. But the execution of those source code blocks also are undeniably "needed to authenticate." Indeed, even Dr. Cole admitted at deposition that, without the push notification received in the App, the authentication process cannot proceed. Ex. 1 at 210:9–23; 233:2–9; 236:15–237:4.

Dr. Cole offers no explanation for this arbitrary distinction between the source code blocks that execute *before* or *after* the "approve" or "deny" selection, or how a skilled artisan could understand where the boundaries of this "software elements needed to authenticate" construction begin and end. The real reason behind Dr. Cole's exclusion of the source code blocks that execute *before* the user's selection is obvious: they execute as a result of *remote* user action (*i.e.*, choosing the "Send Me a Push" option on the computer), not local activation, and thus cannot meet the claim limitation under the Court's claim construction ruling. Dr. Cole should not be permitted to present this legally wrong construction to the jury, which allows the "authentication function" to be anything in software that he wants it to be and would render the claims indefinite.

VI. CONCLUSION

As the Federal Circuit has recognized, "[t]he risk of confusing the jury" already "is high when experts opine on claim construction before the jury." *CytoLogix Corp. v. Ventana Medical Systems, Inc.*, 424 F.3d 1168, 1172 (Fed. Cir. 2005). That risk of jury confusion will be almost certain if Dr. Cole is permitted to present his legally incorrect construction to the jury. His construction and opinions applying it therefore should be excluded.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Jennifer Ying

Jennifer Ying (#5550)
Travis J. Murray (#6882)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jying@morrisnichols.com
tmurray@morrisnichols.com

Attorneys for Defendants Duo Security LLC f/k/a Duo Security, Inc. and Cisco Systems, Inc.

OF COUNSEL:

Brian A. Rosenthal
Katherine Dominguez
Allen Kathir
Hyunjong Ryan Jin
Charlie Sim
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
(212) 351-4000

Jaysen S. Chung
Julian Manasse-Boetani
GIBSON, DUNN & CRUTCHER LLP
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
(415) 393-8200

Nathaniel R. Scharn
GIBSON, DUNN & CRUTCHER LLP
3161 Michelson Drive, Suite 1200
Irvine, CA 92612-4412
(949) 451-3800

December 20, 2024

CERTIFICATE OF SERVICE

I hereby certify that on December 20, 2024, I caused the foregoing to be electronically filed with the Clerk of the Court using CM/ECF, which will send notification of such filing to all registered participants.

I further certify that I caused copies of the foregoing document to be served on December 20, 2024, upon the following in the manner indicated:

David E. Moore, Esquire — *VIA ELECTRONIC MAIL*
Bindu A. Palapura, Esquire
POTTER, ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 North Market Street
Wilmington, DE 19801
Attorneys for Plaintiff

Scott T. Weingaertner, Esquire — *VIA ELECTRONIC MAIL*
Stefan Mentzer, Esquire
John Padro, Esquire
Matthew Wisnieff, Esquire
Lauren Kuehn Pelletier, Esquire
Timothy Francis Keegan, Esquire
GOODWIN PROCTER LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018
Attorneys for Plaintiff

Farzad Feyzi, Esquire — *VIA ELECTRONIC MAIL*
GOODWIN PROCTER LLP
601 Marshall Street
Redwood City, CA 94063
Attorneys for Plaintiff

/s/ Jennifer Ying
Jennifer Ying (#5550)